BOEING SCIENTIFIC RESEARCH LABORATORIES DOCUMENT D1-82-0844

SCIENTIFIC RESEARCH LABORATORIES

Regularities in Congruential Random Number Generators

George Marsaglia

MATHEMATICS RESEARCH

MAY 1969

8

D1-82-0844

REGULARITIES IN CONGRUENTIAL RANDOM NUMBER GENERATORS

by

George Marsaglia

Mathematical Note No. 601

Mathematics Research Laboratory

BOEING SCIENTIFIC RESEARCH LABORATORIES

May 1969

SUMMARY

This paper suggests, as did an earlier one, [1] that points in n-space produced by congruential random number generators are too regular for general Monte Carlo use. Regularity was established in [1] for multiplicative congruential generators by showing that all the points fall in sets of relatively few parallel hyperplanes. The existence of many containing sets of parallel hyperplanes was easily established, but proof that the number of hyperplanes was small required a result of Minkowski from the geometry of numbers--a symmetric, convex set of volume 2^n must contain at least two points with integral coordinates. The present paper takes a different approach to establishing the coarse lattice structure of congruential generators. It gives a simple, self-contained proof that points in n-space produced by the general congruential generator $r_{i+1} \equiv ar_i + b \bmod m$ must fall on a lattice with unit-cell volume at least m^{n-1}. There is no restriction on a or b; this means that *all* congruential random number generators must be considered unsatisfactory in terms of lattices containing the points they produce, for a good generator of random integers should have an n-lattice with unit-cell volume 1.

The Lattice of a Random Number Generator.

Suppose we define the n-*lattice* of a random number generator as follows: if the generator produces integers $r_1,r_2,r_3,\ldots$ let $\pi_1 = (r_1,r_2,\ldots,r_n)$, $\pi_2 = (r_2,r_3,\ldots,r_{n+1}),\ldots$ be the set of possible points in n-space formed from n successive r's. The n-lattice of the generator is the set of all integral linear combinations of points from this set translated to include the origin, i.e., all integral linear combinations of the points

$$\pi_2-\pi_1,\pi_3-\pi_1,\pi_4-\pi_1,\ldots \; . \tag{1}$$

The *unit-cell volume* of the n-lattice is the greatest common iivisor of the volumes of parallelepipeds formed from any $n+1$ points of the lattice; the volume of such a parallelepiped is the determinant with rows formed by subtracting one of the points from each of the other n points.

The unit-cell volume may be considered a generalization of the idea of the greatest common divisor of a set of zero-translated integers, and even a few dozen points in n-space with truly random integer coordinates is virtually certain to have an n-lattice with unit-cell volume 1. The following theorem shows that the lattice structure of every congruential random number generator is far too gross to make the generator suitable for general Monte Carlo use:

THEOREM. *Let*

$$\begin{aligned}
\tau_1 &= (1, T(1), T^2(1), \ldots, T^{n-1}(1)) \\
\tau_2 &= (2, T(2), T^2(2), \ldots, T^{n-1}(2)) \\
&\vdots \\
\tau_m &= (0, T(0), T^2(0), \ldots, T^{n-1}(0))
\end{aligned}$$

be the set of all possible points in n-*space whose coordinates are genrrated successively from an initial coordinate by a linear transformation* T *on the ring of reduced residues of some modulus* m:

$$T(x) \equiv ax + b \mod m \qquad 0 \le T(x) < m,$$

or, using the greatest integer notation,

$$T(x) = ax + b - m[(ax+b)/m].$$

Then all of the points $\tau_1, \tau_2, \ldots, \tau_m$ *lie on a lattice with unit-cell volume* m^{n-1}.

The proof is not very difficult and the case $n = 3$ will serve to describe the general situation. Since the volume of the unit cell of a lattice is the greatest common divisor of the volumes of parallelepipeds formed from sets of $n+1$ points, it suffices to prove that, for any reduced residues r, s, t, v,

$$\begin{vmatrix} r-v & T(r)-T(v) & T^2(r)-T^2(v) \\ s-v & T(s)-T(v) & T^2(s)-T^2(v) \\ t-v & T(t)-T(v) & T^2(t)-T^2(v) \end{vmatrix} \equiv 0 \mod m^{n-1}.$$

Now it is easy to verify that

$$T^j(r) - T^j(v) - a^j(r-v) \equiv 0 \bmod m \tag{2}$$

(since, for example, $T^2(r) = a^2r + ab + b - m[\frac{a^2r+ab+b}{m}]$). Subtracting a^{i-1} times the first column from the i^{th} column, for $i=2,3$ will produce a determinant whose columns, except the first, have m as a factor. In general, then, the determinant will have m^{n-1} as a factor. Since there are m distinct points $\tau_1,\ldots,\tau_m$, the unit-cell volume of their lattice will be exactly m^{n-1}. Points produced by any particular congruential generator will be a subset of the τ's and will have a lattice with unit-cell volume at least m^{n-1}.

Note that, by virtue of (2), every zero-translated point in n-space will have the form

$$(x, ax-ym, a^2x-zm, \ldots)$$

and this form readily provides a basis for the lattice--for example, the rows of this matrix are a basis of the 4-lattice:

$$\begin{pmatrix} 1 & a & a^2 & a^3 \\ 0 & m & 0 & 0 \\ 0 & 0 & m & 0 \\ 0 & 0 & 0 & m \end{pmatrix}.$$

Relation to Sets of Parallel Hyperplanes.

The paper cited above [1] suggested that the crystalline structure of multiplicative congruential generators was too crude by showing that points in n-space produced by such generators must lie in a set of less than $(n!m)^{1/n}$ parallel hyperplanes. The above theorem shows that every congruential generator produces points in n-space which fall on a lattice with unit-cell volume m^{n-1}. To relate the two, imagine the "best possible" lattice, with cubic structure, and with one of the sets of parallel faces perpendicular to the longest line through the cube of points with integer coordinates in the range 0 to m. The length of the diagonal is $m\sqrt{n}$, and the length of a side of the cubic unit-cell is $(m^{n-1})^{1/n}$. Dividing the length of the diagonal, $m\sqrt{n}$, by the distance between parallel hyperplanes, $m^{(n-1)/n}$, we get this bound for the number of hyperplanes containing all the points of a congruential random number generator: $\sqrt{n}\,m^{1/n}$. This, if true, would be an improvement on the previous bound, $(n!m)^{1/n}$. Can the argument be made rigorous? The question is mainly academic, for in either case the bound is too low to make congruential generators suitable for general use.

REFERENCE

[1] George Marsaglia, Random Numbers Fall Mainly in the Planes, *Proc. Nat. Acad. Sci.*, 61, September 1968, pp. 25-28.